Fermat'n pieni lause ja Eulerin lause

Timo Hautamäki

2019/03

Matematiikka
Pro gradu -tutkielma

MATEMAATTIS-LUONNONTIETEELLINEN
TIEDEKUNTA

- HELSINGIN YLIOPISTO -

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Osasto — Avdelning — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen osasto

Tekijä — Författare — Author
Timo Hautamäki

Työn nimi — Arbetets titel — Title

Fermat'n pieni lause ja Eulerin lause

Oppiaine — Läroämne — Subject
Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Maaliskuu 2019	30 s.

Tiivistelmä — Referat — Abstract

Tutkielmassa perehdytään Fermat'n pieneen lauseeseen ja sen todistuksiin. Fermat'n pientä lausetta tarkastellaan myös alkulukutestauksen näkökulmasta. Loppupuolella määritellään Eulerin ϕ-funktio ja esitetään Eulerin lause. Eulerin lauseen käytännöllisyyttä tarkastellaan jakojäännösten selvittämisessä.

Tutkielman johdanto on pieni katsaus Pierre de Fermat'n ja Leonhard Eulerin elämään. Johdannossa käsitellään myös Fermat'n pienen lauseen sekä Eulerin lauseen historiaa. Tutkielmassa on käytetty useita lukuteoreettisia käsitteitä, jotka määritellään heti johdannon jälkeen luvussa Tutkielmassa käytettyjä määritelmiä.

Tutkielma esittää Fermat'n pienen lauseen kolmessa eri muodossa, jotka kaikki ovat keskenään ekvivalentteja. Lauseen käyttöä havainnollistetaan myös muutamalla esimerkillä. Luvussa Fermat'n pienen lauseen todistuksia kyseinen lause todistetaan ensin suoraviivaisesti ja sen jälkeen induktiolla. Lopuksi lausetta havainnollistetaan kuvitellun helminauhan avulla.

Tutkielma osoittaa, että Fermat'n pieni lause toteutuu millä tahansa alkuluvulla p. Fermat'n pienen lauseen toteutuminen jollain luvulla ei kuitenkaan yksin riitä osoittamaan lukua alkuluvuksi. Otsikon Pseudoalkuluvut alla käsitellään lukuja, jotka eivät ole alkulukuja, mutta joilla Fermat'n pieni lause toteutuu.

Jotta voitaisiin varmistua, että luku on alkuluku, E. Lucas kehitti 1800-luvun loppupuolella alkulukutestin, joka hyödyntää Fermat'n pientä lausetta. Testi on esitetty, todistettu ja sitä on havainnollistettu esimerkein kohdassa Lucas-Lehmer alkulukutesti. Testin todistukseen vaaditaan muutamia aputuloksia, jotka on esitetty ennen varsinaista testiä.

Tutkielma määrittelee Eulerin ϕ-funktion ja havainnollistaa sen käyttöä esimerkillä. Tämän jälkeen tutkielmassa johdetaan kaava, jonka avulla ϕ-funktion arvon voi kätevästi laskea. Kaavan johtamista varten on todistettu muutama aputulos. Kaavan käytöstä on esimerkki.

Tutkielmassa käsitellään Eulerin lause. Heti määritelmän jälkeen Eulerin lauseella ratkaistaan jakojäännöksiä. Sitten Eulerin lause todistetaan ensin induktion ja binomikaavan avulla ja sitten redusoidun jäännösluokkasysteemin avulla. Ennen kumpaakin todistusta esitellään ja todistetaan todistuksissa käytettäviä aputuloksia. Lopuksi tutkielma käsittelee suurten potenssien jakojäännösten ratkaisemista Eulerin lauseen ja binäärijärjestelmän avulla.

Avainsanat — Nyckelord — Keywords
Lukuteoria, kongruenssi, ϕ-funktio, Fermat'n pieni lause, Eulerin lause

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

1 Johdanto

Pierre de Fermat (1601-1665) oli ranskalainen lakimies. Vaikka matematiikka oli hänelle vain harrastus, häntä pidetään yhtenä merkittävimmistä 1600-luvulla eläneistä matemaatikoista. Häntä on kutsuttu jopa nimikkeellä harrastelijoiden kuningas. Fermat oli kiinnostunut lukuteoriaan liittyvistä ongelmista. Toisaalta hän jätti merkittävän jäljen myös analyyttisen geometrian, todennäköisyyslaskennan, derivoinnin ja integroinnin historiaan.

Fermat ei mielellään tuonut omia tuotoksiaan julkisuuteen ja siksi hänen töidensä jäljille on päästy vasta hänen kuolemansa jälkeen. Hänellä oli tapana käydä kirjeenvaihtoa muiden matemaatikoiden kanssa ja esitellä kirjeissään uusia keksintöjään. Fermat'n pieni lause, jota tämä kandidaatin tutkielma käsittelee, on todennäköisesti syntynyt Fermat'n tutkiessa täydellisiä lukuja (vuonna 1636). Se on löydetty eräästä hänen kirjeestään, jossa hän esittelee kyseisen lauseen uskotulleen Freniclelle. Fermat jätti kirjeissään lauseidensa todistukset tarkoituksella kirjoittamatta, ja siksi tämäkään kirje ei sisältänyt todistusta. Ensimmäisenä Fermat'n pienen lauseen todisti Gottfried Wilhelm Leibniz (1646-1716) todennäköisesti ennen vuotta 1683.

Myöhemmin Fermat'n pieneen lauseeseen paneutui sveitsiläissyntyinen Leonhard Euler (1707-1783). Eulerin isä oli ammatiltaan pappi ja toivoi myös pojastaan pappia. Jo lapsena Euler lähti seuraamaan isänsä tahdosta tämän jalanjälkiä Baselin yliopistoon. Papinura sai kuitenkin käänteen, kun Baselin yliopiston matematiikan professori Johann Bernoulli (1667-1748) huomasi Eulerin olevan poikkeuksellisen lahjakas matematiikassa. Euler sai Bernoullilta matematiikan opetusta joka lauantai-iltapäivä ja kehittyi näin matematiikassa. Kun Bernoulli tajusi, miten suuri matemaatikko Eulerista voisi tulla, hän pyysi tämän isältä hyväksyntää uranvaihdolle. Tällöin Eulerin isä luopui poikaansa liittyvistä teologisista tavoitteistaan ja Eulerin tie jatkui virallisesti matematiikan parissa. Hän valmistui maisteriksi 17-vuotiaana ja 19-vuotiaana häneltä ilmeistyi kaksi väitöstutkimusta.

Merkittävän osan matemaatiikon urastaan Euler teki Venäjällä ja Saksassa. Ollessaan 26-vuotias hän sai johtavan matemaatikon paikan Pietarin yliopistosta. Venäjällä ollessaan hän alkoi myös käydä kirjeenvaihtoa Christian Goldbachin (1690-1764) kanssa. Goldbach oli Eulerille ikään kuin matemaattinen mentori, joka tutustutti Eulerin geometriaan ja lukuteoriaan Fermat'n töiden kautta. Venäjällä ollessaan hän kehitteli Fermat'n pienestä lauseesta omia versioitaan ja todisti niitä. 1750-luvulla Saksassa ollessaan hän todisti Fermat'n pienen lauseen sellaisenaan ja kehitti siitä myös yleisemmän muodon, joka nimettiin hänen itsensä mukaan: Eulerin lauseen.

Tämä tutkielma sisältää Fermat'n pienen lauseen muotoilun sekä lauseeseen liittyviä esimerkkejä ja todistuksia. Lisäksi tutkielma käsittelee lausetta alkulukutestauksen näkökulmasta. Tutkielma osoittaa, että pseudoluvut sekä erityisesti Carmichaelin luvut ovat alkulukutestauksessa Fermat'n pienen lauseen so-

keita pisteitä. Myöhemmin 1800-luvulla Edouard Lucas kehitti testin, jossa Fermat'n pientä lausetta käytetään aputuloksena. Testi julkaistiin kuitenkin vasta 1900-luvulla D. H. Lehmerin ansiosta. Tutkielma käsittelee Lucas-Lehmerin alkulukutestiä todistuksen ja kahden esimerkin avulla.

Todistaessaan Fermat'n pientä lausetta Euler kehitti tietynlaisille luvuille funktion, jota hän alkoi merkitä π-kirjaimella. Hän julkaisi funktion vuonna 1763. Myöhemmin Carl Friedrich Gauss (1777-1855) muutti funktion kirjaimeksi ϕ. Tutkielma määrittelee Eulerin lauseen sisältämän ϕ-funktion ja sille johdetaan myös kaava. ϕ-funktion käytöstä on myös esimerkit. Kun ϕ-funktio on määritelty, tutkielmassa tarkastellaan Eulerin lausetta jakojäännösten selvityksen näkökulmasta. Eulerin lauseelle esitetään myös kaksi todistusta, toinen induktion ja binomikaavan avulla ja toinen redusoidun jäännösluokkasysteemin avulla. Lopuksi tutkielma esittelee menetelmän suurten potenssien jakojäännösten selvittämiseen. Menetelmässä hyödynnetään Eulerin lausetta ja binäärijärjestelmää.

2 Tutkielmassa käytettyjä määritelmiä

Määritellään aluksi tutkielmassa käytettyä käsiteistöä.

Määritelmä 1. *Olkoon luvut a ja b kokonaislukuja. Luku a on jaollinen luvulla b, jos on olemassa kokonaisluku c, jolla pätee $a = c \cdot b$.*

Määritelmä 2. *Olkoon luvut a ja b kokonaislukuja. Luku a on luvun b tekijä, jos on olemassa kokonaisluku c, jolla pätee $b = c \cdot a$. Tällöin myös luku c on luvun b tekijä.*

Määritelmä 3. *Olkoon luvut a ja b kokonaislukuja. Lukujen a ja b suurin yhteinen tekijä on suurin sellainen kokonaisluku c, joka on sekä luvun a että luvun b tekijä. Tällöin merkitään $\text{syt}(a, b) = c$.*

Määritelmä 4. *Olkoon p positiivinen ja lukua 1 suurempi kokonaisluku. Luku p on alkuluku, jos se on jaollinen ainoastaan luvulla 1 sekä itsellään.*

Määritelmä 5. *Olkoon p positiivinen ja lukua 1 suurempi kokonaisluku. Luku p on yhdistetty luku, jos ja vain jos on olemassa luvusta 1 poikkeavat kokonaisluvut a ja b, joilla $p = a \cdot b$. Toisin sanoen p on yhdistetty luku, mikäli se ei ole alkuluku.*

Määritelmä 6. *Olkoon luvut a ja b kokonaislukuja. Luku a on luvun b alkutekijä, mikäli luku a on alkuluku ja mikäli se on luvun b tekijä.*

Määritellään seuraavaksi kongruenssirelaatio.

Määritelmä 7. *Olkoon luvut a, b ja c kokonaislukuja. Olkoon lisäksi $c \neq 0$. Mikäli on olemassa kokonaisluku k, jolla pätee*

$$\begin{aligned} a &= k \cdot c + b \\ a - b &= k \cdot c \\ b - a &= -k \cdot c \\ b &= -k \cdot c + a, \end{aligned}$$

ovat luvut a ja b keskenään kongruentit modulo c. Tämä merkitään

$$a \equiv b \pmod{c}.$$

Mikäli a ja b eivät ole kongruentit, merkitään $a \not\equiv b \pmod{c}$.

Havainnollistetaan tätä vielä lukuesimerkillä.

Esimerkki 1. Osoitetaan, että $52 \equiv 12 \pmod{10}$.

Luvut 52 ja 12 ovat keskenään kongruentit modulo 10, sillä

$$52 = 4 \cdot 10 + 12 \text{ ja toisaalta } 12 = -4 \cdot 10 + 52.$$

Määritelmä 8. *Olkoon n positiivinen kokonaisluku. Sanotaan, että joukko A on täydellinen jäännösluokkasysteemi* $(\mathrm{mod}\ n)$*, jos joukossa A on tasan n alkiota ja mitkään kaksi joukon A alkiota eivät ole keskenään kongruentit modulo n. Tällöin jokainen joukon A alkio on kongruentti tasan yhden joukon $\{0, 1, 2, ..., n-1\}$ alkion kanssa.*

Esimerkki 2. Onko joukko $H = \{-8, -2, 9, 15\}$ on täydellinen jäännösluokkasysteemi modulo 4? Huomaamme, että joukossa H on tasan 4 alkiota. Lisäksi

$$-8 \equiv 0, 9 \equiv 1, -2 \equiv 2, 15 \equiv 3 \pmod 4.$$

Siispä kukin joukon H alkio on kongruentti tasan yhden joukon $\{0, 1, 2, 3\}$ alkion kanssa. Siispä H on täydellinen jäännösluokkasysteemi modulo 4.

Määritelmä 9. *Olkoon a ja b kokonaislukuja. Lukuja a ja b kutsutaan keskenään jaottomiksi kokonaisluvuiksi tai suhteellisiksi alkuluvuiksi, mikäli*

$$syt(a, b) = 1.$$

Määritelmä 10. *Olkoon a ja b keskenään jaottomia kokonaislukuja. Olkoon lisäksi $b > 1$. Luvun a kertaluku modulo b on pienin positiivinen kokonaisluku n, jolla*

$$a^n \equiv 1 \pmod b.$$

3 Fermat'n pieni lause

Esitetään seuraavaksi Fermat'n pieni lause.

Lause 1. *Olkoon a kokonaisluku ja p alkuluku ja olkoon luvut a ja p keskenään jaottomia. Tällöin pätee*

$$a^p \equiv a \pmod{p}.$$

Lause voidaan kirjoittaa myös muodossa

$$a^{p-1} \equiv 1 \pmod{p}$$

tai muodossa, jossa Fermat sen kirjeessään ilmoitti:

Seuraus 1. *Luku p jakaa luvun $a^{p-1} - 1$ aina, kun p on alkuluku ja a ja p ovat keskenään jaottomia kokonaislukuja.*

Havainnollistetaan Fermat'n pienen lauseen käyttöä muutamalla esimerkillä.

Esimerkki 3. Luku 7 on alkuluku. Nyt

$$2^7 = 128 = 126 + 2 = 18 \cdot 7 + 2 \equiv 2 \pmod{7}.$$

Esimerkki 4. Luku 5 on alkuluku. Nyt

$$3^5 = 243 = 240 + 3 = 48 \cdot 5 + 3 \equiv 3 \pmod{5}.$$

Esimerkki 5. Etsitään Fermat'n pienen lauseen avulla luvun 2^{242} pienin jakojäännös modulo 19. Koska

$$2^{242} = (2^{18})^{16}$$

ja tiedämme Fermat'n pieneen lauseen nojalla, että

$$2^{18} \equiv 1 \pmod{19},$$

saamme Apulauseen 2 (s. 13) nojalla

$$2^{242} \equiv (2^{18})^{16} \equiv 1^{16} \equiv 1 \pmod{19}.$$

4 Fermat'n pienen lauseen todistuksia

Seuraavaksi käymme läpi kaksi Fermat'n pienen lauseen todistusta sekä havainnollistamme lausetta kuvitellun helminauhan avulla.

4.1 Suoraviivainen todistus

Todistus. Olkoon p alkuluku ja a sellainen kokonaisluku, ettei se ole jaollinen luvulla p. Olkoon meillä myös positiivisten kokonaislukujen osajoukko

$$T = \{1, 2, 3, ..., (p-1)\}.$$

Koska alkuluku p ei ole luvun a eikä toisaalta mikään joukon T alkion tekijä, niin ei mikään jokainen joukon $T_a = \{a, 2a, 3a, ..., (p-1)a\}$ alkiokaan voi olla jaollinen luvulla p.

Tästä seuraa, että jokainen joukon T alkio on kongruentti täsmälleen yhden joukon T_a alkion kanssa ja päinvastoin. Eli mikäli $ma \equiv na \pmod{p}$, niin silloin pätee myös $m \equiv n \pmod{p}$. Tästä seuraa, että mitkään luvuista

$$a, 2a, 3a, ..., (p-1)a$$

eivät ole keskenään kongruentteja modulo p.

Nyt tiedämme, että varmasti

$$1 \cdot 2 \cdot ... \cdot (p-1) \equiv a \cdot 2a \cdot ... \cdot (p-1)a \pmod{p}$$

ja edelleen, että

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}.$$

Koska p ei ole luvun $(p-1)!$ tekijä, voidaan lauseke jakaa puolittain luvulla $(p-1)!$ Tästä saamme Fermat'n pienen lauseen

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

4.2 Todistus induktion avulla

Todistetaan Fermat'n pieni lause seuraavaksi induktiolla hyödyntäen binomikaavaa.

Todistus. Olkoon p alkuluku. Ensimmäiseksi toteamme, että Fermat'n pieni lause pätee nollalla. Koska tiedämme, että $0^p = 0$, niin varmasti myös $0^p \equiv 0 \pmod{p}$.

Oletetaan seuraavaksi, että $a^p \equiv a \pmod{p}$ pätee jollain kokonaisluvulla a. Tällöin oletamme myös, että $a^p - a \equiv 0 \pmod{p}$. Koska Fermat'n pienen lauseen $a^p \equiv a \pmod{p}$ tulee päteä mielivaltaisella kokonaisluvulla a, osoitamme, että mikäli Fermat'n lause pätee kokonaisluvulla a, se pätee myös kokonaisluvuilla

$a-1$ sekä $a+1$. Eli oletetaan seuraavaksi, että $a^p \equiv a \pmod{p}$ pätee jollain kokonaisluvulla a ja osoitetaan, että tällöin pätee myös

$$(a-1)^p \equiv a-1 \pmod{p}$$

sekä

$$(a+1)^p \equiv a+1 \pmod{p}.$$

Ajatellaan seuraavaksi binomikerrointa $\binom{p}{k}$. Se on jaollinen luvulla p, sillä

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)...(p-k+1)\cdot(p-k)!}{k!(p-k)!} = \frac{p(p-1)...(p-k+1)}{k!}.$$

Tällöin myös luvut

$$\binom{p}{1}, \binom{p}{2}, ..., \binom{p}{p-1}$$

ovat jaollisia luvulla p.

Binomikaavan avulla tiedämme, että

$$(a \pm 1)^p = \binom{p}{0}a^p \pm \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} \pm ... + \binom{p}{p-1}a \pm \binom{p}{p}.$$

Tästä saamme edelleen

$$(a \pm 1)^p - a^p \mp 1 = \pm\binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} \pm ... + \binom{p}{p-1}a.$$

Huomaamme, että yhtälön oikealla puolella jokainen termi ja siten koko yhtälön oikea puoli on jaollinen luvulla p. Tällöin myös vasemman puolen on oltava jaollinen luvulla p, eli saamme

$$(a \pm 1)^p - a^p \mp 1 \equiv 0 \pmod{p}.$$

Oletimme induktio-oletuksena, että $a^p - a$ on jaollinen luvulla p. Voimme nyt lisätä yhtölän vasemmalle puolelle luvun $a^p - a$ tietäen, että jakojäännös ei muutu. Lisäyksen jälkeen pätee

$$(a \pm 1)^p - a^p \mp 1 + a^p - a \equiv 0 \pmod{p}$$

ja sievennettynä

$$(a \pm 1)^p \mp 1 - a \equiv 0 \pmod{p}.$$

Muokataan lauseke vielä muotoon, jota lähdimme todistuksessa tavoittelemaan:

$$(a \pm 1)^p \equiv a \pm 1 \pmod{p}.$$

Olemme siis alussa osoittaneet, että Fermat'n pieni lause pätee kokonaisluvulla 0. Tämän jälkeen osoitimme induktiolla, että mikäli lauseke
$a^p \equiv a \pmod{p}$ pätee jollain kokonaisluvulla a, se pätee myös, mikäli luku a korvataan luvulla $(a-1)$ tai $(a+1)$. Täten Fermat'n lause $a^p \equiv a \pmod{p}$ pätee kaikilla kokonaisluvuilla a luvun p ollessa alkuluku, mikä oli todistettava. $\square$

4.3 Fermat'n pieni lause helminauhan avulla

Kuvitellaan, että rakennamme helminauhoja. Meillä on käytössämme erivärisiä helmiä. Olkoon värejä a kappaletta ja olkoon kunkin värisiä helmiä käytettävissä rajaton määrä. Tarkoituksenamme on rakentaa helminauhoja, joihin tulee aina p kappaletta helmiä ja tarkoitus on vieläpä rakentaa niin monta erilaista helminauhaa kuin vain suinkin on mahdollista. Helminauhoissa on etukäteen määritetyt paikat helmille: ensimmäinen helmi, toinen helmi, ..., $(p-1)$. helmi ja p. helmi. Nyt kaksi helminauhaa ovat samanlaiset vain, jos niiden ensimmäiset helmet, toiset helmet jne... ovat keskenään samanväriset.

Ensimmäinen kysymys on, montako erilaista helminauhaa pystymme muodostamaan. Helminauhan ensimmäiselle paikalle on a kappaletta ehdokkaita, samoin kaikille muillekin paikoille. Koska paikkoja on yhteensä p kappaletta ja jokaiselle valitaan helmi a:sta erivärisestä, voimme muodostaa yhteensä a^p erilaista helminauhaa.

Koska meillä on a kappaletta erilaisia värejä, voimme muodostaa tasan a kappaletta yksivärisiä, keskenään erivärisiä helminauhoja. Koska kaikkia mahdollisia helminauhoja on a^p kappaletta ja niistä yksivärisiä on a kappaletta, monivärisiä vaihtoehtoja on oltava tällöin $a^p - a$ kappaletta.

Oletetaan, että olemme nyt muodostaneet kaikki mahdolliset helminauhat ja poistaneet joukosta kaikki yksiväriset helminauhat. Poimimme seuraavaksi yhden monivärisen helminauhan ja muodostamme siitä uusia helminauhoja siten, että siirrämme ensimmäisen paikan helmen toiselle paikalle, toisen helmen paikan kolmannelle ja lopulta viimeisen helmen ensimmäiselle paikalle. Saatuamme uuden helminauhan voimme toistaa saman operaation uudestaan ja uudestaan, kunnes jokainen helmi on kiertänyt kaikki paikat. Pystymme muodostamaan poimimallamme helminauhalla siis p kappaletta keskenään erilaisia helminauhoja. Koska olemme jo luoneet kaikki erilaiset helminauhat ja koska toisaalta nyt tiedämme, että millä tahansa niistä pystyy luomaan tasan p kappaletta keskenään erilaisia helminauhoja, huomaamme, että voimme ryhmitellä kaikki moniväriset helminauhat ryhmiin, joihin kuuluu kuhunkin p helminauhaa. Koska monivärisiä helminauhoja on $a^p - a$ kappaletta ja tämä luku on jaollinen luvulla p, saamme Fermat'n pienen lauseen:

$$a^p - a \equiv 0 \pmod{p}.$$

5 Pseudoalkuluvut

Jos luku p on alkuluku, Fermat'n pieni lause toteutuu kaikilla kokonaisluvuilla a. Tästä seuraa, että mikäli a on kokonaisluku ja Fermat'n pieni lause ei toteudu, luku p ei ole alkuluku.

Sen perusteella, että Fermat'n pieni lause toteutuu ja a on kokonaisluku, emme voi kuitenkaan todeta lukua p alkuluvuksi. On olemassa myös yhdistettyjä lukuja, jotka toteuttavat Fermat'n pienen lauseen.

Määritelmä 11. *Lukua p, joka ei ole alkuluku, mutta toteuttaa Fermat'n pienen lauseen muodossa*

$$2^p \equiv 2 \pmod{p},$$

kutsutaan pseudoalkuluvuksi.

Pseudoalkuluvun kriteeri siis on, että se on yhdistetty ja toteuttaa Fermat'n pienen lauseen, kun $a = 2$. Mikäli se toteuttaa Fermat'n pienen lauseen kaikilla kokonaisluvuilla a, kutsutaan sitä Carmichaelin luvuksi.

Määritelmä 12. *Lukua p, joka ei ole alkuluku, mutta toteuttaa kuitenkin kaikilla kokonaisluvuilla a Fermat'n pienen lauseen*

$$a^p \equiv a \pmod{p},$$

kutsutaan Carmichaelin luvuksi.

Esimerkki 6. Osoita, että luku 1105 on pseudoalkuluku.

Todistus. Tiedämme, että $1105 = 5 \cdot 13 \cdot 17$. Koska luvut $5, 13$ ja 17 ovat alkulukuja, ne toteuttavat Fermat'n pienen lauseen. Siksi tiedämme, että

$$2^4 \equiv 1 \pmod{5},$$

$$2^{12} \equiv 1 \pmod{13}$$

ja

$$2^{16} \equiv 1 \pmod{17}.$$

Nyt Apulauseen 2 (s. 13) nojalla

$$2^{1104} \equiv (2^4)^{276} \equiv 1^{276} \equiv 1 \pmod{5},$$

$$2^{1104} \equiv (2^{12})^{92} \equiv 1^{92} \equiv 1 \pmod{13}$$

sekä

$$2^{1104} \equiv (2^{16})^{69} \equiv 1^{69} \equiv 1 \pmod{17}.$$

Siispä luku $2^{1104} - 1$ on jaollinen luvuilla 5, 13 ja 17. Koska nämä luvut ovat alkulukuja ja toisaalta luvun 1105 alkutekijät, on luvun $2^{1104}-1$ oltava jaollinen myös luvulla 1105. Koska siis pätee

$$2^{1104} - 1 \equiv 0 \pmod{1105},$$

toteuttaa yhdistetty luku 1105 pseudoalkuluvun kriteerit. □

6 Lucas-Lehmerin alkulukutesti

Ennen Lucas-Lehmerin alkulukutestiä käymme läpi muutaman lauseen, joita kyseisen testin todistamiseen tarvitaan.

6.1 Todistuksessa käytettäviä apulauseita

Lause 2. ***(Eulerin lause)*** *Olkoon $a \in \mathbb{Z}$ ja syt$(a, b) = 1$. Tällöin*

$$a^{\phi(b)} \equiv 1 \pmod{b}.$$

Todistus. Lause todistetaan luvussa 9. □

Huomautus. $\phi(b)$ kuvaa niiden positiivisten kokonaislukujen lukumäärää, jotka ovat lukua b pienempiä ja suhteellisia alkulukuja luvun b kanssa. ϕ-funktio määritellään luvussa 7.

Apulause 1. *Olkoon p positiivinen kokonaisluku. Tällöin*

$$\phi(p) = p - 1$$

jos ja vain jos p on alkuluku.

Todistus. Oletetaan, että p on alkuluku ja osoitetaan, että

$$\phi(p) = p - 1.$$

Koska $\phi(p)$ kuvaa niiden alkioiden määrää, jotka ovat pienempiä kuin luku p, ei niiden määrä voi olla yhtä suuri tai suurempi kuin p. Tällöin on oltava $\phi(p) < p$.

Mikäli $\phi(p) < p - 1$, olisi joukossa $\{1, 2, ..., p - 1\}$ oltava vähintään yksi luku a, joka ei olisi suhteellinen alkuluku luvun p kanssa. Tällöin pätisi syt$(a, p) > 1$, mistä seuraisi, että luvulla p olisi lukua 1 suurempi ja toisaalta itseään pienempi tekijä. Päädymme ristiriitaan, sillä p olisi tällöin yhdistetty luku.

On siis osoitettu, että mikäli p on alkuluku, pätee

$$\phi(p) = p - 1.$$

Oletetaan sitten, että pätee

$$\phi(p) = p - 1$$

ja osoitetaan, että luvun p on oltava alkuluku.

Tehdään vastaoletus: oletetaan, että luku p on yhdistetty luku. Nyt tiedämme, että luvulla p on olemassa ainakin kaksi lukua yhtä suurempaa ja lukua p pienempää tekijää a ja b, joilla pätee $p = a \cdot b$.

Koska oletimme, että $\phi(p) = p - 1$, on kaikkien lukua p pienempien positiivisten kokonaislukujen oltava suhteellisia alkulukuja luvun p kanssa. Toisaalta tiedämme, että luvut a ja b ovat lukua 1 suurempia ja lukua p pienempiä positiivisia kokonaislukuja, mutta ne eivät kuitenkaan ole suhteellisia alkulukuja luvun p kanssa, päädymme ristiriitaan. Siis luvun p on oltava alkuluku.

□

Apulause 2. *Olkoon $a \equiv b \pmod{c}$. Nyt kaikilla $n \in \mathbb{N}$ pätee*

$$a^n \equiv b^n \pmod{c}.$$

Todistetaan väite induktiolla.

Todistus. Alkuaskel: Olkoon $n = 0$. Nyt $a^0 = 1$ ja $b^0 = 1$. Koska

$$1 \equiv 1 \pmod{c},$$

lause pätee, kun $n = 0$.

Induktio-askel: Oletamme seuraavaksi, että

$$a^n \equiv b^n \pmod{c}$$

ja osoitamme, että tällöin pätee myös

$$a^{n+1} \equiv b^{n+1} \pmod{c}.$$

Nyt

$$a^{n+1} - b^{n+1} = a \cdot a^n - b \cdot b^n.$$

Tiedämme, että $a = b + kc$ jollakin kokonaisluvulla k. Tästä seuraa, että

$$a \cdot a^n - b \cdot b^n = (b + kc) \cdot a^n - b \cdot b^n = b(a^n - b^n) + kc \cdot a^n.$$

Induktio-oletuksesta seuraa, että $a^n - b^n = tc$ jollakin kokonaisluvulla t. Siispä

$$b(a^n - b^n) + kc \cdot a^n = btc + kc \cdot a^n = c(bt + ka^n).$$

Koska siis

$$a^{n+1} - b^{n+1} = c(bt + ka^n)$$

eli luku $(a^{n+1} - b^{n+1})$ on jaollinen luvulla c, on lukujen a^{n+1} ja b^{n+1} oltava kongruentit modulo c.

Siispä kaikilla $n \in \mathbb{N}$ pätee

$$a^n \equiv b^n \pmod{c}.$$

□

Apulause 3. *Olkoon kokonaisluku k kokonaisluvun a kertaluku modulo p. Tällöin*

$$a^t \equiv 1 \pmod{p}$$

jos ja vain jos t on jaollinen luvulla k.

Todistus. Todistetaan ensin, että mikäli $a^t \equiv 1 \pmod{p}$, niin t on jaollinen luvulla k ja sen jälkeen toiseen suuntaan.

Tiedetään, että positiivinen kokonaisluku k on luvun a kertaluku modulo p. Oletetaan lisäksi $a^t \equiv 1 \pmod{p}$. Koska k on luvun a kertaluku, on oltava $k \leq t$. Täten t on muotoa $sk + c$ joillakin $s, c \in \mathbb{Z}$. Lisäksi $0 \leq c < k$.

Nyt Apulauseen 2 nojalla

$$a^t = a^{sk+c} = a^{sk}a^c = (a^k)^s a^c \equiv 1^s a^c = a^c \pmod{p}.$$

Jos $c = 0$, niin silloin $a^c = a^0 = 1$ ja tällöin saamme, että $a^t \equiv 1 \pmod{p}$.

Mikäli $0 < c < k$, päädymme ristiriitaan, sillä k on pienin sellainen positiivinen kokonaisluku x, joka toteuttaa yhtälön $a^x \equiv 1 \pmod{p}$. Koska $c < k$, ei voi olla $a^c \equiv 1 \pmod{p}$.

Tästä seuraa, että $r = 0$, jolloin $t = sk + 0 = sk$. Siispä t on jaollinen luvulla k.

Oletetaan seuraavaksi, että t on jaollinen luvulla k. Tällöin on olemassa sellainen kokonaisluku s, jolla pätee $t = sk$. Siispä Apulauseen 2 nojalla saamme

$$a^t = a^{sk} = (a^k)^s \equiv 1^s = 1 \pmod{p}$$

eli $a^t \equiv 1 \pmod{p}$. □

Seuraus 2. *Olkoon luvut a ja $p > 0$ kokonaislukuja. Jos luku k on luvun a kertaluku modulo p ja jos $\text{syt}(a, p) = 1$, niin $\phi(p)$ on jaollinen luvulla k.*

Todistus. Lauseen 2 avulla saamme, että $a^{\phi(p)} \equiv 1 \pmod{p}$ ja Apulauseen 3 avulla, että $\phi(p)$ on jaollinen luvulla k. □

6.2 Lucasin alkulukutesti

Määrittelemme seuraavasti Lucasin alkulukutestin.

Lause 3. *Jos on olemassa sellainen kokonaisluku a, jolla pätee Fermat'n pieni lause*

$$a^{p-1} \equiv 1 \pmod{p}$$

ja lisäksi kaikilla luvun $(p-1)$ alkutekijöillä q pätee

$$a^{(p-1)/q} \not\equiv 1 \pmod{p},$$

niin p on alkuluku.

Todistus. Olkoon a, k ja n kokonaislukuja ja olkoon k luvun a kertaluku modulo n. Nyt Määritelmän 10 avulla tiedämme, että $\text{syt}(a, p) = 1$ ja että k on pienin mahdollinen positiivinen kokonaisluku, jolla pätee

$$a^k \equiv 1 \pmod{p}.$$

Tästä seuraa Apulauseen 3 avulla, että $p-1$ on jaollinen luvulla k ja siten on olemassa $s \in \mathbb{Z}$, jolla $p-1 = sk$. Mikäli $s > 1$, niin sillä olisi olemassa alkutekijä q, jolla $s = ql$ jollakin kokonaisluvulla l. Silloin myös $p - 1 = qlk$. Nyt pätisi

$$a^{p-1/q} = a^{lk} = (a^k)^l \equiv 1^l = 1 \pmod{p},$$

mikä on ristiriita oletuksen $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ kanssa.

Eli $s = 1$ ja Seurauksen 3 avulla tiedämme myös, että $\phi(p)$ on jaollinen luvulla k. Nyt luvun kertaluku k ei voi olla suurempi kuin luku $\phi(p)$, joka on jaollinen luvulla k. Nyt siis

$$p - 1 = k \leq \phi(p) = p - 1$$

eli $\phi(p) = p - 1$. Siispä Apulauseen 1 nojalla p on alkuluku.

□

Esimerkki 7. Tutkitaan, onko luku 17 alkuluku.

Olkoon $a = 3$. Nyt Fermat'n pieni lause toteutuu, sillä

$$a^{16} = 3^{16} = 43046721 = 43046721 + 1 = 2532160 \cdot 17 + 1 \equiv 1 \pmod{17}.$$

Tarkastetaan seuraavaksi, päteekö kaikilla luvun $17 - 1 = 16$ alkutekijöillä q

$$3^{16/q} \not\equiv 1 \pmod{17}.$$

Tiedämme, että luvun 16 ainoa alkutekijä on 2, sillä $2^4 = 16$. Nyt saamme

$$3^{16/2} = 3^8 = 6561 = 385 \cdot 17 + 16 \not\equiv 1 \pmod{17}.$$

Koska luvun $17 - 1$ ainoa alkutekijä on $q = 2$ ja se ei toteuta yhtälöä

$$a^{16/q} \equiv 1 \pmod{17},$$

on luvun 17 oltava alkuluku.

Esimerkki 8. Osoitetaan, että luku 341 on pseudoalkuluku Lucasin alkulukutestin avulla.

Fermat'n lause toteutuu, kun $a = 2$, sillä

$$2^{341-1} = 2^{340} = (2^{10})^{34} = 1024^{34} = (3 \cdot 341 + 1)^{34}.$$

Apulauseen 2 avulla

$$(3 \cdot 341 + 1)^{34} \equiv 1^{34} \equiv 1 \pmod{341}.$$

Nyt tiedämme, että luku 341 toteuttaa Fermat'n pienen lauseen, joten se on joko alkuluku tai pseudoalkuluku.

Luvun $341 - 1$ alkutekijät ovat 17, 5 ja 2, sillä

$$341 - 1 = 340 = 17 \cdot 20 = 17 \cdot 5 \cdot 2 \cdot 2.$$

Olkoon $q = 17$. Nyt

$$2^{340/17} = 2^{20} = (2^{10})^2.$$

Yllä saimme, että $2^{10} \equiv 1 \pmod{341}$, joten Apulauseen 2 nojalla

$$2^{340/17} = 2^{20} = (2^{10})^2 \equiv 1^2 \equiv 1 \pmod{341}.$$

Koska löydettiin luvun $341 - 1$ alkutekijä q, joka toteuttaa yhtälön

$$2^{340/17} \equiv 1 \pmod{341},$$

luku 341 on pseudoalkuluku.

7 ϕ -funktio

Määritellään seuraavaksi Eulerin lauseessa käytettävä ϕ-funktio.

7.1 Maaritelma

Määritelmä 13. *Olkoon n positiivinen kokonaisluku. Funktio $\phi(n)$ on niiden positiivisten kokonaislukujen lukumäärä, jotka ovat lukua n pienempiä ja toisaalta suhteellisia alkulukuja luvun n kanssa.*

Havainnollistetaan tätä vielä esimerkillä.

Esimerkki 9. Olkoon $n = 26$. Listataan seuraavaksi kaikki lukua 26 pienemmät positiiviset kokonaisluvut k, jotka toteuttavat ehdon $syt(k, n) = 1$. Luvuksi k kelpaavat kaikki seuraavan joukon alkiot:

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Koska joukossa on 12 alkiota, saamme $\phi(n) = 12$.

7.2 ϕ-funktion kaava

Apulause 4. *Olkoon a, n keskenään jaottomat positiiviset kokonaisluvut. Olkoon lisäksi joukko $\{c_1, c_2, \cdots, c_n\}$ täydellinen jäännösluokkasysteemi modulo n. Tällöin joukko*

$$\{ac_1 + b, ac_2 + b, \cdots, ac_n + b\}$$

on myös täydellinen jäännösluokkasysteemi modulo n millä tahansa kokonaisluvulla b.

Todistus. Huomaamme, että joukossa

$$D = \{ac_1 + b, ac_2 + b, \cdots, ac_n + b\}$$

on tasan n alkiota. Riittää siis osoittaa, että mitkään kaksi joukon D alkiota eivät ole keskenään kongruentteja modulo n.

Olkoon $g, h \in \{1, 2, \cdots, n\}$. Oletetaan, että luvut $ac_g + b$ ja $a, c_h + b$ ovat keskenään kongruentit modulo n. Tällöin myös pätee $ac_g \equiv ac_h \pmod{n}$.

Kongruenssin määritelmän avulla tiedämme, että

$$ac_g - ac_h = sn, s \in \mathbb{Z}$$

eli

$$ac_g - ac_h \equiv 0 \pmod{n}$$

ja edelleen

$$a(c_g - c_h) \equiv 0 \pmod{n}.$$

Koska a ja n ovat keskenään jaottomia, on oltava $c_g - c_h \equiv 0 \pmod{n}$ ja kongruenssin määritelmän nojalla $c_g \equiv c_h \pmod{n}$.

Koska joukko $\{c_1, c_2, \cdots, c_n\}$ on täydellinen jäännösluokkasysteemi, on oltava $c_g = c_h$. Tällöin myös $ac_g + b = ac_h + b$ eli joukon D kaksi alkiota ovat keskenään kongruentit modulo n vain, jos ne ovat sama alkio. Siispä joukko D on täydellinen jäännösluokkasysteemi modulo n. □

Lause 4. *Olkoon luvut m ja n keskenään jaottomia positiivia kokonaislukuja. Tällöin $\phi(mn) = \phi(m)\phi(n)$ eli ϕ on multiplikatiivinen.*

Todistus. Olkoon meillä joukko $J = \{A_1 \cup A_2 \cup \cdots \cup A_m\}$, jossa

$$A_1 = \{1, m+1, 2m+1, \cdots, (n-1)m+1\},$$

$$A_2 = \{2, m+2, 2m+2, \cdots, (n-1)m+2\},$$

$$A_3 = \{3, m+3, 2m+3, \cdots, (n-1)m+3\}, \cdots$$

$$A_m = \{m, 2m, 3m, \cdots, nm\}.$$

Joukko J sisältää siis alkiot $1, 2, \cdots, mn$.

Olkoon meillä nyt $k \in \{1, 2, \cdots, m\}$. Tällöin

$$A_k = \{k, m+k, 2m+k, \cdots, (n-1)m+k\}$$

Jos luvuilla m ja k on yhteinen tekijä $c > 1$, niin varmasti myös $am + k$ on jaollinen luvulla c millä tahansa $a \in 1, 2, \cdots, (n-1)$. Siispä kaikki joukon A_k alkiot ovat jaollisia luvulla c.

Jos haluamme löytää joukosta A_k suhteellisia alkulukuja luvun mn kanssa, tulee meidän siis olettaa, että m ja k ovat keskenään jaottomat. Tällöin myös kaikki joukon A_k alkiot ovat suhteellisia alkulukuja luvun m kanssa. Koska lisäksi luvut $0, 1, \cdots, n-1$ muodostavat täydellisen jäännösluokkasysteemin modulo n, myös joukon A_k alkiot muodostavat täydellisen jäännösluokkasysteemin modulo n (Apulause 4). Tällöin joukon $\{0, 1, \cdots, n-1\}$ tavoin on myös joukossa A_k oltava $\phi(n)$ kappaletta suhteellisia alkulukuja luvun n kanssa. Tällöin nämä luvut ovat suhteellisia alkulukuja myös tulon mn kanssa, sillä kaikki joukon A_k alkiot ovat oletettu suhteellisiksi alkuluvuiksi luvun m kanssa. Tiedämme, että joukossa $\{1, 2, \cdots, m\}$ on $\phi(m)$ kappaletta sellaisia lukuja, jotka ovat suhteellisia alkulukuja luvun m kanssa. Samoin joukkoperheessä $\{A_1, A_2, \cdots, A_m\}$ on $\phi(m)$ kappaletta sellaisia joukkoja, joiden alkiot ovat suhteellisia alkulukuja luvun m kanssa. Jokaisessa näistä joukoista on $\phi(n)$ kappaletta lukuja, jotka ovat suhteellisia alkulukuja luvun mn kanssa. Siispä $\phi(mn) = \phi(m)\phi(n)$ ja ϕ on multiplikatiivinen. □

Lause 5. *Olkoon p alkuluku ja olkoon $k \in \mathbb{Z}_+$. Tällöin*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

Todistus. Koska p on alkuluku, tiedämme, että $syt(p^k, a) = 1$ jos ja vain jos p ei ole luvun a tekijä. Lisäksi tiedämme, että lukujen $1, 2, \cdots, p^k$ joukosta vain kaikki luvun p monikerrat ovat jaollisia luvulla p. Nämä luvut ovat $p, 2p, 3p, \cdots, (p^{k-1}p)$. Toisin sanoen p^k:sta luvusta joka p:s on jaollinen luvulla p. Tällöin näitä lukuja on $\frac{p^k}{p} = p^{k-1}$ kappaletta. Loput $p^k - p^{k-1}$ lukua eivät ole jaollisia luvulla p ja ovat siis suhteellisia alkulukuja luvun p^k kanssa.

Siispä

$$\phi(p^k) = p^k - p^{k-1} = p^k - \frac{p^k}{p} = p^k(1 - \frac{1}{p}).$$

□

Todistetaan edellisten lauseiden pohjalta ϕ-funktion kaava.

Lause 6. *Olkoon $n \in \mathbb{Z}_+$ ja $k_1, k_2, \cdots, k_i \in \mathbb{Z}_+$. Ajatellaan, että luku n on jaettu alkutekijöihinsä $p_1, p_2, \cdots, p_i$, missä $p_s = p_t$ jos ja vain jos $s = t$ ($s, t \in \{1, 2, \cdots, i\}$). Ilmoitetaan n alkutekijöidensä potenssien tulona $n = p_1^{k_1}, p_2^{k_2}, \cdots, p_i^{k_i}$. Tällöin*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot \cdots \cdot (1 - \frac{1}{p_i}).$$

Todistus. Lauseessa 4 osoitetun ϕ-funktion multiplikatiivisuuden nojalla

$$\phi(n) = \phi(p_1^{k_1}), \phi(p_2^{k_2}), \cdots, \phi(p_i^{k_i}).$$

Toisaalta edellisen lauseen nojalla voimme ilmoittaa millä tahansa $s \in \{1, 2, \cdots, i\}$ luvun $\phi(p_s^{k_s})$ muodossa $p_s^{k_s}(1 - \frac{1}{p_s})$.

Niinpä saamme

$$\phi(n) = p_1^{k_1}(1-\frac{1}{p_1})p_2^{k_2}(1-\frac{1}{p_2}) \cdots p_i^{k_i}(1-\frac{1}{p_i}) = p_1^{k_1}p_2^{k_2} \cdots p_i^{k_i}(1-\frac{1}{p_1})(1-\frac{1}{p_2}) \cdots (1-\frac{1}{p_i}).$$

Kun sijoitamme $p_1^{k_1}p_2^{k_2} \cdots p_i^{k_i} = n$, saamme halutun muodon

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_i}).$$

□

Lasketaan seuraavaksi vielä Esimerkki 9 käyttäen äsken todistettua ϕ-funktion kaavaa.

Esimerkki 10. Lasketaan funktion $\phi(n)$ arvo, kun $n = 26$. Luvun 26 alkutekijät ovat luvut 2 ja 13.

Tällöin

$$\phi(26) = 26(1 - \frac{1}{2})(1 - \frac{1}{13}) = 26 \cdot \frac{1}{2} \cdot \frac{12}{13} = 26 \cdot \frac{12}{26} = 12.$$

8 Eulerin lause

Eulerin lause esitettiin jo luvussa 6, mutta kerrataan se tässä yhteydessä.

Olkoon $a \in \mathbb{Z}$ ja $\text{syt}(a, n) = 1$. Tällöin

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Samalla huomaamme, että mikäli n on alkuluku, kaikki lukua n pienemmät positiiviset kokonaisluvut ovat suhteellisia alkulukuja luvun n kanssa. Siispä $\phi(n) = n - 1$. Tällöin Eulerin lause tulee muotoon $a^{n-1} \equiv 1 \pmod{n}$, mikä on Fermat'n pieni lause. Toisin sanoen Fermat'n pieni lause on muuten kuin Eulerin lause, mutta luvun n on oltava alkuluku. Eulerin lauseen ehto $syt(a, n)$ toteutuu väistämättä, mikäli n on alkuluku ja se ei jaa lukua a.

Havainnollistetaan Eulerin lauseen käyttöä kahdella esimerkillä.

Esimerkki 11. Laske jakolaskun $\dfrac{7^{494}}{26}$ jakojäännös.

Koska luku 7 on alkuluku eikä ole luvun 26 tekijä, on sen myös oltava suhteellinen alkuluku luvun 26 kanssa. Siispä voimme käyttää Eulerin lausetta arvoilla $a = 7, n = 26$. Lasketaan

$$\phi(26) = 26(1 - \frac{1}{2})(1 - \frac{1}{13}) = 26 \cdot \frac{1}{2} \cdot \frac{12}{13} = 26 \cdot \frac{12}{26} = 12.$$

Tällöin $7^{494} \equiv x \pmod{26}$, missä x on kysytty jakojäännös.

Koska $494 = 12 \cdot 41 + 2$, saadaan $7^{494} = (7^{12})^{41} \cdot 7^2 = (7^{\phi(26)})^{41} \cdot 7^2$. Nyt siis Eulerin lauseen nojalla

$$(7^{\phi(26)})^{41} \cdot 7^2 \equiv 1^{41} \cdot 7^2 \equiv 7^2 \equiv 49 \equiv 26 + 23 \equiv 23 \pmod{26}.$$

Jakolaskun $\dfrac{7^{494}}{26}$ jakojäännös on siis 23.

Esimerkki 12. Osoita Eulerin lauseen avulla, että $9^{60n+2} \equiv 20 \pmod{61}$ kaikilla $n \in \mathbb{Z}$.

Koska luku 61 on alkuluku, on $\phi(61) = 61 - 1 = 60$. Lisäksi luvut 9 ja 61 ovat keskenään jaottomat. Nyt

$$9^{60n+2} = (9^{60})^n \cdot 9^2 = (9^{\phi(61)})^n \cdot 9^2.$$

Eulerin lauseen nojalla $9^{\phi(61)} \equiv 1 \pmod{61}$. Siispä

$$(9^{\phi(61)})^n \cdot 9^2 \equiv 1^n \cdot 9^2 \equiv 9^2 \equiv 81 \equiv 20 \pmod{61}.$$

On osoitettu, että $9^{60n+2} \equiv 20 \pmod{61}$ kaikilla $n \in \mathbb{Z}$.

9 Eulerin lauseen todistuksia

9.1 Todistus induktion ja binomikaavan avulla

Ennen kuin todistamme Eulerin lauseen induktion avulla, todistamme binomikaavan yleisen muodon.

Lause 7. *Olkoot $a, b \in \mathbb{R}$ ja $n \in \mathbb{Z}_+$. Tällöin*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Todistus. Osoitetaan binomikaava oikeaksi induktiolla. Otetaan ensimmäinen askel ja osoitetaan että se pätee, kun $n = 1$. Saamme

$$(a+b)^1 = \sum_{i=0}^{1} \binom{1}{i} a^i b^{1-i} = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = 1 \cdot 1 \cdot b + 1 \cdot a \cdot 1 = a + b.$$

Koska arvolla $n = 1$ binomikaava on tosi, voimme tehdä induktio-oletuksen. Oletamme todeksi binomikaavan millä tahansa luvulla $n \in \mathbb{Z}_+$ ja osoitamme, että tällöin binomikaava toteutuu myös luvulla $n+1$. Induktio oletuksen nojalla siis $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

Osoitetaan, että

$$(a+b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.$$

Nyt $(a+b)^{n+1} = (a+b)(a+b)^n$ ja induktio-oletuksesta saamme edelleen

$$(a+b)(a+b)^n = (a+b) \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Kertomalla tämän auki, saamme lausekkeen muotoon

$$\sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1}.$$

Asetetaan ensimmäisen summafunktion luku i käymään läpi luvut $1, 2, ..., n+1$ ja korvataan kaikki kyseisen termin i:t luvulla $i-1$. Tällöin saamme lausekkeen

$$\sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n-(i-1)} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1} = \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n-i+1} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1}.$$

Koska on sovittu, että $\binom{n}{-1} = 0$, ei ole väliä, alkaako ensimmäinen summa luvusta 0 vaiko luvusta 1. Muutetaan se siis alkamaan nollasta, jotta voimme yhdistää kaiken yhden summafunktion alle. Siispä

$$\sum_{i=0}^{n+1} \binom{n}{i-1} a^i b^{n-i+1} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1} = \sum_{i=0}^{n+1} \left[\binom{n}{i-1} + \binom{n}{i} \right] a^i b^{n-i+1}.$$

Sievennetään $\binom{n}{i-1} + \binom{n}{i}$ mieluisaan muotoon

$$\begin{aligned}
\binom{n}{i-1} + \binom{n}{i} &= \frac{n!}{(i-1)!(n-i+1)!} + \frac{n!}{i!(n-i)!} \\
&= \frac{n!i!(n-i)! + n!(i-1)!(n-i+1)!}{(i-1)!(n+1-i)!i!(n-i)!} \\
&= \frac{n!(i!(n-i)! + (i-1)!(n-i+1)!)}{(n-i)!(i-1)!(n+1-i)!i!} \\
&= \frac{n!(i! + (i-1)!(n-i+1))}{(i-1)!(n+1-i)!i!} \\
&= \frac{n!(i + (n-i+1))}{i!(n+1-i)} \\
&= \frac{n!(n+1))}{i!(n+1-i)} \\
&= \frac{(n+1)!}{i!(n+1-i)} \\
&= \binom{n+1}{i}.
\end{aligned}$$

Siispä saamme

$$\sum_{i=0}^{n+1} \left[\binom{n}{i-1} \binom{n}{i} \right] a^i b^{n-i+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i},$$

$$\text{eli } (a+b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i} \text{ on tosi.}$$

Olemme todistaneet binomikaavan induktiolla.

□

Osoitamme seuraavaksi Eulerin lauseen induktiolla.

Lause 8. *Olkoon $a \in \mathbb{Z}$ ja $syt(a, n) = 1$. Tällöin*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Todistus. Olkoon p alkuluku ja $a, k \in \mathbb{Z}$. Olkoon lisäksi $k > 0$ ja olkoot p ja a keskenään suhteellisia alkulukuja. Osoitetaan, että tällöin $a^{\phi(p^k)} \equiv 1 \pmod{p^k}$.

Otetaan ensimmäinen askel eli $k = 1$. Nyt saamme Fermat'n pienen lauseen

$$a^{\phi(p)} = a^{p-1} \equiv 1 \pmod{p}.$$

Koska olemme aiemmin jo todistaneet Fermat'n pienen lauseen, väite on tosi arvolla $k = 1$.

Tehdään seuraavaksi induktio-oletus ja oletetaan, että osoitettava väite on tosi, kun $k = n$ jollain $n \in \mathbb{Z}_+$. Oletamme siis, että

$$a^{\phi(p^n)} \equiv 1 \pmod{p^n}.$$

Otetaan induktioaskel ja osoitetaan, että

$$a^{\phi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}.$$

Koska p on alkuluku, voimme käyttää Lausetta 5. Saamme

$$\phi(p^{n+1}) = p^{n+1} - p^n.$$

Ottamalla luvun p yhteiseksi tekijäksi ja hyödyntämällä jälleen Lausetta 5 saamme ϕ-funktion muuttujan induktio-oletuksen hyödyntämisen kannalta tärkeään muotoon

$$p^{n+1} - p^n = p(p^n - p^{n-1}) = p\phi(p^n).$$

Induktio-oletuksen pohjalta voimme päätellä, että jollakin $s \in \mathbb{Z}$

$$a^{\phi(p^n)} = sp^n + 1.$$

Näiden tietojen pohjalta

$$a^{\phi(p^{n+1})} = a^{p\phi(p^n)} = (a^{\phi(p^n)})^p = (sp^n + 1)^p.$$

Soveltamalla binomikaavaa (Lause 7) saamme

$$\begin{aligned}
(sp^n + 1)^p &= \sum_{i=0}^{p} \binom{p}{i} (sp^n)^{p-i} \cdot 1^{p-i} \\
&= \sum_{i=0}^{p} \binom{p}{i} (sp^n)^{p-i} \\
&= \binom{p}{0}(sp^n)^{p-0} + \binom{p}{1}(sp^n)^{p-1} + \cdots + \binom{p}{p-1}(sp^n)^{p-p+1}\binom{p}{p}(sp^n)^{p-p} \\
&= (sp^n)^p + p(sp^n)^{p-1} + \binom{p}{2}(sp^n)^{p-2} + \cdots + p(sp^n) + 1.
\end{aligned}$$

Havaitsemme, että ensimmäinen termi $(sp^n)^p$ on jaollinen luvulla pp^n. Samalla kaikki muutkin termit, lukuunottamatta viimeistä termiä, ovat jaollisia luvulla p^{n+1}, sillä kaikki näiden termien kombinaatiot jakavat luvun p (todistettu luvussa 4.2) ja kaikista termeistä löytyy p^n. Siispä

$$(sp^n)^p + p(sp^n)^{p-1} + \binom{p}{2}(sp^n)^{p-2} + \cdots + p(sp^n) + 1 \equiv 1 \pmod{p^{n+1}}.$$

Olemme todistaneet induktiolla, että

$$a^{\phi(p^n)} \equiv 1 \pmod{p^n}.$$

Oletetaan seuraavaksi, että a ja m ovat keskenään suhteellisia alkulukuja ja $m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$. Koska m ja a eivät ole keskenään jaollisia, ei myös mikään luvun m tekijä $p_j^{n_j}$, missä $j \in \{1, 2, \cdots r\}$, voi olla muuta kuin suhteellinen alkuluku luvun a kanssa. Voimme siis käyttää induktio-todistuksen tulosta ja saamme

$$a^{\phi(p_j^{n_j})} \equiv 1 \pmod{p_j^{n_j}}.$$

Koska ϕ on multiplikatiivinen ja siten

$$\phi(m) = \phi(p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}) = \phi(p_1^{n_1})\phi(p_2^{n_2}) \cdots \phi(p_r^{n_r}),$$

on luvun $\phi(p_j^{n_j})$ oltava luvun $\phi(m)$ tekijä. Voimme korottaa yhtälön

$$a^{\phi(p_j^{n_j})} \equiv 1 \pmod{p_j^{n_j}}$$

molemmat puolet potenssiin $\dfrac{\phi(n)}{\phi(p_j^{n_j})}$. Lauseke

$$a^{\phi(p_j^{n_j})\frac{\phi(n)}{\phi(p_j^{n_j})}} \equiv 1^{\frac{\phi(n)}{\phi(p_j^{n_j})}} \pmod{p_j^{n_j}}$$

sievenee haluttuun muotoon

$$a^{\phi(n)} \equiv 1 \pmod{p_j^{n_j}}.$$

Koska tiedämme, että millä tahansa $j \in \{1, 2, \cdots r\}$ pätee

$$a^{\phi(n)} \equiv 1 \pmod{p_j^{n_j}},$$

voimme päätellä, että

$$a^{\phi(n)} - 1 \text{ on jaollinen millä tahansa } p_j^{n_j}.$$

Lisäksi, koska millä tahansa $j, v \in \{1, 2, \cdots r\}$ pätee $syt(p_j^{n_j}, p_v^{n_v}) = 1$, on oltava

$$a^{\phi(n)} \equiv 1 \pmod{(p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r})}$$

ja edelleen

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Olemme todistaneet Eulerin lauseen induktiolla.

□

9.2 Todistus redusoidun jäännösluokkasysteemin avulla

Ennen kuin todistamme Eulerin lauseen, määrittelemme redusoidun jäännösluokkasysteemin käsitteen ja havainnollistamme sitä esimerkillä.

Määritelmä 14. *Olkoon $a, b, n \in \mathbb{Z}$. Joukko A on redusoitu jäännösluokkasysteemi modulo n, jos siinä on $\phi(n)$ alkiota, jos kaikilla $a \in A$ pätee $syt(a, n) = 1$ ja jos millään $a, b \in A$ ei ole $a \equiv b \pmod{n}$.*

Seuraus 3. *Olkoon joukko A niiden alkioiden joukko, joiden lukumäärää $\phi(n), n \in \mathbb{Z}_+$, kuvaa. Tällöin A on redusoitu jäännösluokkasysteemi.*

Todistus. Huomaamme, että joukossa A on $\phi(n)$ alkiota ja nämä alkiot ovat jokainen ϕ-funktion määritelmän mukaan luvun n kanssa keskenään jaottomia. Koska lisäksi mitkään kaksi A:n alkiota eivät ollessaan välillä $1, 2, \cdots n-1$ voi olla keskenään kongruentteja modulo n, niin A on redusoitu jäännösluokkasysteemi. □

Esimerkki 13. Tutkitaan, onko joukko $J = \{1, 19, 23, 47\}$ redusoitu jäännösluokkasysteemi modulo 10.

Lasketaan ensin, onko $\phi(10) = 4$. Välillä $1, 2, \cdots 9$ luvun 10 tekijät ovat 2 ja 5. Saamme ϕ-funktion kaavasta

$$\phi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 10 \cdot \frac{4}{10} = 4.$$

Huomaamme, että $1 \equiv 1, 19 \equiv 9, 23 \equiv 3$ ja $47 \equiv 7 \pmod{10}$. Lisäksi

$$syt(1, 10) = syt(19, 10) = syt(23, 10) = syt(47, 10) = 1,$$

joten J on redusoitu jäännösluokkasysteemi.

Apulause 5. *Olkoon a ja b kokonaislukuja ja p alkuluku. Olkoon myös p tulon ab tekijä. Tällöin p on myös luvun a tai luvun b tekijä.*

Todistus. Luvut a ja b voidaan ilmoittaa alkutekijöidensä potensseina seuraavasti:

$$a = p_{a_1}^{j_1} p_{a_2}^{j_2} \cdots p_{a_m}^{j_m} \text{ ja } b = p_{b_1}^{k_1} p_{b_2}^{k_2} \cdots p_{b_n}^{k_n}.$$

Samoin tulon ab voimme ilmoittaa muodossa

$$ab = p_{a_1}^{j_1} p_{b_1}^{k_1} p_{a_2}^{j_2} p_{b_2}^{k_2} \cdots p_{a_m}^{j_m} p_{b_n}^{k_n}.$$

Koska p on tulon ab tekijä, sen on kuuluttava joukkoon $\{p_{a_1}, p_{b_1}, p_{a_2}, p_{b_2}, \cdots, p_{a_m} p_{b_n}\}$. Tällöin se kuuluu myös joukkoon $\{p_{a_1}^{j_1} p_{a_2}^{j_2} \cdots p_{a_m}^{j_m}\}$ tai $\{p_{b_1}^{k_1} p_{b_2}^{k_2} \cdots p_{b_n}^{k_n}\}$, jotka ovat luvun a ja b alkutekijät. Siispä p on luvun a tai b tekijä. □

Lause 9. *Olkoon joukko* $\{r_1, r_2, \cdots, r_{\phi(n)}\}$ *redusoitu jäännösluokkasysteemi modulo* n*. Olkoon lisäksi* $a \in \mathbb{Z}_+$ *keskenään jaoton luvun* n *kanssa. Tällöin myös joukko* $\{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ *on redusoitu jäännösluokkasysteemi modulo* n*.*

Todistus. Huomaamme, että joukossa $\{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ on tasan $\phi(n)$ alkiota. Jotta se olisi redusoitu jäännösluokkasysteemi, meidän tulee vielä osoittaa, että mikä tahansa ar_j, missä $j \in \{1, 2, \cdots, \phi(n)\}$, on keskenään jaoton luvun n kanssa ja etteivät mitkään kaksi joukon $\{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ alkioista ole keskenään kongruentteja modulo n.

Osoitetaan ensin, että mikä tahansa $ar_j, j \in \{1, 2, \cdots, \phi(n)\}$, on keskenään jaoton luvun n kanssa.

Tehdään vastaoletus: $syt(ar_j, n) = c > 1$. Koska c jakaa luvun n lisäksi tulon ar_j, on Apulauseen 5 mukaan myös vähintään toisen luvuista a ja r_j oltava jaollinen luvulla c. Koska alussa oletuksena oli, että $syt(a, n) = 1$, ei voi olla olemassa lukua c, joka jakaa sekä luvun n että luvun a. Toisaalta r_j ja n ovat keskenään jaottomat, koska r_j kuuluu redusoituun jäännösluokkasysteemiin modulo n. Siispä ei ole olemassa $c > 1$, jolla $syt(a, n) = c$ tai $syt(r_j, n) = c$ eli on oltava $syt(ar_j, n) = 1$.

Osoitetaan vielä, että mitkään kaksi joukon $\{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ alkioista eivät ole keskenään kongruentteja modulo n.

Tehdään taas vastaoletus: on olemassa $s, t \in \{1, 2, \cdots, \phi(n)\}$ siten, että $s \neq t$ ja kuitenkin $ar_s \equiv ar_t \pmod{n}$. Tällöin kongruenssin määritelmän nojalla $ar_s - ar_t = a(r_s - r_t) = qn$ jollain $q \in \mathbb{Z}$. Toisaalta tiedämme, että $syt(a, n) = 1$, joten Apulauseen 5 mukaan erotuksen $r_s - r_t$ on oltava jaollinen luvulla n. Tämä ei kuitenkaan ole mahdollista, koska r_s ja r_t kuuluvat redusoituun jäännösluokkasysteemiin modulo n. Päädymme ristiriitaan ja siksi mitkään kaksi joukon $\{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ alkioista eivät ole keskenään kongruentteja modulo n. □

Todistetaan seuraavaksi Eulerin lause redusoidun jäännösluokkasysteemin avulla.

Lause 10. *Olkoon* $a \in \mathbb{Z}$ *ja* $syt(a, n) = 1$*. Tällöin*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Todistus. Olkoon joukko $R = \{r_1, r_2, \cdots, r_{\phi(n)}\}$ redusoitu jäännösluokkasysteemi modulo n, missä $r_j \in \mathbb{Z}_+$ ja $r_j < n$ kaikilla $j \in \{1, 2, \cdots \phi(n)\}$. Tiedämme, että a ja n ovat keskenään jaottomat, joten tiedämme Lauseen 9 nojalla, että myös joukko $A = \{ar_1, ar_2, \cdots, ar_{\phi(n)}\}$ on redusoitu jäännösluokkasysteemi modulo n.

Osoitetaan seuraavaksi, että joukon R alkiot ovat joukon A pienimmät positiiviset jakojäännökset modulo n. Otetaan joukosta A mikä tahansa alkio ar_j ja olkoon alkio $c \in \mathbb{Z}, 0 \leq c < n$, sen pienin positiivinen jakojäännös modulo n eli $ar_j \equiv c \pmod{n}$. Luku b on joukon R alkio, jos ja vain jos se on suhteellinen

alkuluku luvun n kanssa. Osoitetaan siis, että $syt(b, n) = 1$. Tehdään vastaoletus ja oletetaan, että on olemassa positiivinen luku $h > 1$, joka jakaa sekä luvun n että luvun b. Tällöin taas $ar_j = kn + b$ jollakin $k \in \mathbb{Z}$, jolloin myös luvun ar_j tulisi olla jaollinen luvulla h. Koska ar_j ja n ovat keskenään jaottomat, molemmat eivät voi olla jaollisia luvulla h. Siispä $b \in R$.

Nyt tiedämme, että jokaista joukon A alkiota ar_{s_a} vastaa jokin joukon R alkio $r_s, s \in \{1, 2, \cdots \phi(n)\}$, jolla $ar_{s_a} \equiv r_s$. Tällöin tiedetään kongruenssin laskusääntöjen nojalla, että jos $ar_{s_a} \equiv r_s \pmod{n}$ ja $ar_{t_a} \equiv r_t \pmod{n}$ joillakin $s, t \in \{1, 2, \cdots \phi(n)\}$, pätee myös tulolla $ar_{s_a} ar_{t_a} \equiv r_s r_t \pmod{n}$. Tällä periaatteella saamme lopulta

$$ar_1 ar_2 \cdots ar_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}.$$

Sievennämme tämän muotoon

$$a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}.$$

Nyt siis luku $a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} - r_1 r_2 \cdots r_{\phi(n)} = (a^{\phi(n)} - 1) r_1 r_2 \cdots r_{\phi(n)}$ jakaa luvun n. Koska kaikki joukon R alkiot ovat suhteellisia alkulukuja luvun n kanssa, on luvun $a^{\phi(n)-1}$ oltava jaollinen luvulla n. Tällöin saamme Eulerin lauseen

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Olemme osoittaneet Eulerin lauseen redusoidun jäännösluokkasysteemin avulla.

□

10 Eulerin lause ja suuret potenssit

Jakojäännöksiä voidaan ratkaista myös hyvin isojen potenssien kohdalla. Seuraavaksi tutustumme erääseen menetelmään ensin yleisellä tasolla ja sitten esimerkin kautta.

Olkoon meillä luku a^h, missä $a, h \in \mathbb{Z}_+$ ja h on iso eksponentti. Olkoon lisäksi $syt(a, n) = 1$. Yritämme selvittää jakojäännöstä, kun luku a^h jaetaan luvulla n. Toisin sanoen yritämme selvittää sellaisen luvun $j \in \{0, 1, 2, \cdots, n-1\}$, jolla $a^h \equiv j \pmod{n}$. Koska luku h on jokin iso eksponentti, on se järkevää ilmoittaa muodossa $h = s\phi(n) + r$. Tällöin saamme, että

$$a^s\phi(n) + r = (a^{\phi(n)})^s \cdot a^r.$$

Koska Eulerin lauseen nojalla $a^{\phi(n)} \equiv 1 \pmod{n}$, saamme

$$(a^{\phi(n)})^s \cdot a^r \equiv 1^s \cdot a^r \equiv a^r \pmod{n}.$$

Siispä $a^h \equiv a^r \pmod{n}$.

Tehdään luvusta r binääriesitys. Olkoon $b_j \in \{0, 1\}$, missä $j \in \{0, 1, 2, \cdots, k\}$ ja $b_k = 1$. Saamme binääriesityksen

$$r = b_k \cdot 2^k + b_{k-1} \cdot 2^{k-1} + \cdots + b_1 \cdot 2 + b_0.$$

Olkoon jäännösluokka $[a_i] \pmod{n}$ joukko, johon kuuluvat kaikki ne luvut, jotka ovat muotoa $a_i + km, k \in \mathbb{Z}$. Toisin sanoen jäännösluokka modulo m muodostuu kaikista niistä mahdollisista luvuista, jotka ovat kongruentit keskenään modulo m. Selvitämme seuraavaksi kaikki jäännösluokat $[a_1, a_2, \cdots, a_k] \pmod{n}$. Valitaan kunkin jäännösluokan edustajaksi pienin epänegatiivinen edustaja. Tällöin edustajat ovat välillä $[0, (m-1)]$.

Saamme aina seuraavan jäännösluokan edustajan selville korottamalla edellisen edustajan toiseen potenssiin. Aloitamme luvusta a_1. Olkoon se kongruentti luvun a neliön kanssa modulo n. Siispä $a_1 \equiv a^2 \pmod{n}$. Nyt

$$\begin{aligned}
a_2 &\equiv (a_1)^2 = (a^2)^2 = a^4 = a^{2^2} \pmod{n} \\
a_3 &\equiv (a_2)^2 = (a^{2^2})^2 = a^{2^2 \cdot 2} = a^{2^3} \pmod{n} \\
a_4 &\equiv (a_3)^2 = (a^{2^3})^2 = a^{2^3 \cdot 2} = a^{2^4} \pmod{n} \\
&\cdots \\
a_k &\equiv (a_{k-1})^2 = (a^{2^{k-1}})^2 = a^{2^{k-1} \cdot 2} = a^{2^k} \pmod{n}.
\end{aligned}$$

Tästä saamme

$$\begin{aligned}
a^h \equiv a^r &= a^{b_k \cdot 2^k + b_{k-1} \cdot 2^{k-1} + \cdots + b_1 \cdot 2 + b_0} \\
&= a^{b_k \cdot 2^k} \cdot a^{b_{k-1} \cdot 2^{k-1}} \cdots a^{b_1 \cdot 2} \cdot a^{b_0} \\
&= (a^{2^k})^{b_k} \cdot (a^{2^{k-1}})^{b_{k-1}} \cdots (a^2)^{b_1} \cdot a^{b_0} \pmod{n}.
\end{aligned}$$

Siispä $a^h \equiv (a^{2^k})^{b_k} \cdot (a^{2^{k-1}})^{b_{k-1}} \cdots (a^2)^{b_1} \cdot a^{b_0} \pmod{n}$.

Seuraavaksi valotamme, miten edellisen tuloksen avulla a^h saadaan nopeasti laskettua.

Esimerkki 14. Lasketaan jakojäännös, kun $23^{123456789}$ jaetaan luvulla 599. Tiedämme, että luvut 23 ja 599 ovat alkulukuja. Siispä ne ovat keskenään jaottomat. Voimme soveltaa Eulerin lausetta ehdoilla $a = 23, n = 599$. Tiedämme Apulauseen 1 avulla, että $\phi(599) = 598$. Lisäksi tiedämme, että $h = 123456789 = 206449 \cdot 598 + 287$. Saamme, että $23^{123456789} \equiv 23^{287} \pmod{599}$.

Muodostetaan luvusta 287 binääriesitys

$$287 = 256+16+8+4+2+1 = 1\cdot 2^8+0\cdot 2^7+0\cdot 2^6+0\cdot 2^5+1\cdot 2^4+1\cdot 2^3+1\cdot 2^2+1\cdot 2^1+1\cdot 2^0.$$

Saamme, että $b_8 = b_4 = b_3 = b_2 = b_1 = b_0 = 1$ ja $b_7 = b_6 = b_5 = 0$.

Lasketaan peräkkäisillä neliöönkorotuksilla $a_1, a_2, \cdots, a_8$:

$$\begin{aligned}
a &= 23 \\
a_1 &\equiv a^2 \equiv 23^2 = 529 \pmod{599} \\
a_2 &\equiv a_1^2 \equiv 529^2 = 279841 \equiv 108 \pmod{599} \\
a_3 &\equiv a_2^2 \equiv 108^2 = 11664 \equiv 283 \pmod{599} \\
a_4 &\equiv a_3^2 \equiv 283^2 = 80089 \equiv 422 \pmod{599} \\
a_5 &\equiv a_4^2 \equiv 422^2 = 178084 \equiv 181 \pmod{599} \\
a_6 &\equiv a_5^2 \equiv 181^2 = 32761 \equiv 415 \pmod{599} \\
a_7 &\equiv a_6^2 \equiv 415^2 = 172225 \equiv 312 \pmod{599} \\
a_8 &\equiv a_7^2 \equiv 312^2 = 97344 \equiv 306 \pmod{599}.
\end{aligned}$$

Ratkaisemme nyt luvun $23^{123456789}$ jakojäännöksen.

$$\begin{aligned}
23^{123456789} &\equiv 23^{287} \pmod{599} \\
&\equiv (a_8)^{b_8} \cdot (a_7)^{b_7} \cdot (a_6)^{b_6} \cdot (a_5)^{b_5} \cdot (a_4)^{b_4} \cdot (a_3)^{b_3} \cdot (a_2)^{b_2} \cdot (a_1)^{b_1} \cdot a^{b_0} \pmod{599} \\
&= 306^1 \cdot 312^0 \cdot 415^0 \cdot 181^0 \cdot 422^1 \cdot 283^1 \cdot 108^1 \cdot 529^1 \cdot 23^1 \\
&= (306 \cdot 422) \cdot (283 \cdot 108) \cdot (529 \cdot 23) \\
&\equiv 347 \cdot 15 \cdot 187 \pmod{599} \\
&\equiv 559 \pmod{599}.
\end{aligned}$$

Siispä luvun $23^{123456789}$ jakojäännös on 559, kun se jaetaan luvulla 599.

11 Lähdeluettelo

Viitteet

[1] Rosen, K. H. *Elementary Number Theory and Its Applications. Addison-Wesley Publishing Company, New Jersey. 1993*

[2] Burton, D. M. *Elementary Number Theory, Sixth Edition. McGraw-Hill, New York. 2007*

[3] Boyer, C.B. *A History of Mathematics. Princeton University Press, New Jersey. 1985*

[4] Hintikka, Pekka. *Fermat'n suuri lause, salaisuus kolmen vuosisadan takaa. Gummerus 2003*

[5] Singh, Simon. *Fermat'n viimeinen teoreema. (Fermat's Enigma. The Epic Quest to Solve the World's Greatest Mathematical Problem) Suom. Katriina Savolainen. Tammi 1998*

[6] Bell, E.T. *Men of mathematics. Published by Simon & Schuster, Inc. New York*

[7] Debnath, Lokenath. *The Legacy Of Leonhard Euler: A Tricentennial Tribute. Imperial College Press 2010*

[8] Wikipedia - Fermat'n pieni lause.
`https://fi.wikipedia.org/wiki/Fermat'n_pieni_lause`

[9] Wikipedia - Fermat's little theorem.
`https://en.wikipedia.org/wiki/Fermat's_little_theorem`

[10] Vesalainen, Esa J. *Lyhyt johdatus alkeelliseen lukuteoriaan*
`http://matematiikkakilpailut.fi/kirjallisuus/laajalukuteoriamoniste.pdf`

[11] Mathematical assosiation of America - Math Origins: The Totient Funktion
`https://www.maa.org/press/periodicals/convergence/math-origins-the-totient-function`

[12] Keränen, Teeriaho (RAMK, 2006) - Salausmenetelmät
`http://algebra.fi/keranen/Salausmenetelmat2006/Kappaleet1-4kokonaisina/salausmenetelmat_4eulerinjafermatnlauseet.pdf`